National Infrastructure Protection Center
CyberNotes

Issue #10-99 *May 12, 1999*

CyberNotes is published every two weeks by the National Infrastructure Protection Center (NIPC). Its mission is to support security and information system professionals with timely information on cyber vulnerabilities, hacker exploit scripts, hacker trends, virus information, and other critical infrastructure-related best practices.

You are encouraged to share this publication with colleagues in the information and infrastructure protection field. Electronic copies are available on the NIPC Web site at http://www.nipc.gov.

Please direct any inquiries regarding this publication to the Editor-CyberNotes, National Infrastructure Protection Center, FBI Building, Room 11719, 935 Pennsylvania Avenue, NW, Washington, DC, 20535.

Bugs, Holes & Patches

The following table provides a summary of software vulnerabilities identified between April 24 and May 9, 1999. The table provides the hardware/operating system, equipment/software name, potential vulnerability/impact, identified patches/workarounds/alerts, common name of the vulnerability, potential risk, and an indication of whether attacks have utilized this vulnerability or an exploit script is known to exist. Software versions are identified if known. **This information is presented only as a summary; complete details are available from the source of the patch/workaround/alert, indicated in the footnote or linked site.** Please note that even if the method of attack has not been utilized or an exploit script is not currently widely available on the Internet, a potential vulnerability has been identified. **Updates from previous issues of CyberNotes are listed in bold.**

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
America Online[1]	AIM	Sending a specific hyperlink in the form of aim:addbuddy?=screenname and having the receiver click on the hyperlink will cause the client to crash.	No workarounds or patches known at time of publishing.	AIM Denial-of-Service	Low	Bug discussed in newsgroups and Web sites. Exploit script has been published. Web site has been set up to execute this vulnerability.

[1] BUGTRAQ, April 19, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Computer Software manufaktur[2]	CSMMail	Buffer overflow conditions exist in the "VRFY" and "RCPT TO:" commands that will allow an unauthorized user to execute arbitrary commands.	No workarounds or patches known at time of publishing.	CSMMail remote buffer overflow	**High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
DiscusWare[3]	Discus	The software creates a directory with the permissions 666. In this directory are the files users.txt and admin.txt which contain passwords.	Workaround is to check permissions and make sure the directory has correct permissions (not readable from the web).	Discus directory permissions	**High** (large number of sites potentially vulnerable)	Bug discussed in newsgroups and Web sites. Exploit script not required, web search may reveal vulnerable sites.
FTP Serv-U[4]	FTP Serv-U (v2.5)	FTP Serv-U will crash if 155 or more characters are sent via a command that accepts parameters.	New version of FTP Serv-U corrects this problem. The author has posted reportedly post the fix at: ftp://ftp.cat-soft.com/beta/ but the editor was unable to connect to this site.	FTP Serv-U 155 character problem	Low	Bug discussed in newsgroups and Web sites. Exploit script not required.
Hummingbird[5]	Exceed (V5)	Exceed X allows inbound TCP connection on port 6000. If a SDM host is use to telnet to port 6000 the X server will lock-up.	Version 6.1 appears to correct this problem.	Exceed Denial-of-Service	Low	Bug discussed in newsgroups and Web sites. Exploit script not required.
JDEdwards Enterprise software[6]		Applications have hardcoded passwords. The applications in question appear to install as SECOFR on AS/400s and ADMIN on NT/UNIX systems.	No workarounds or patches known at time of publishing.	JDEdwards hardcoded passwords	**High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Microsoft Windows 95/98[7]	Operating System	A malicious Java program can cause the system to continue to open threads resulting in a Denial-of-Service condition.	Microsoft spokesperson indicated that in order to correct the problem, the relevant code would require "a major overhaul."	Windows 95/98 Java thread problem	Low	Bug discussed in newsgroups and Web sites.
Network Associates[8]	VirusScan NT (v4.0.2)	Due to a suspected race condition, VirusScan may not update virus signatures. The application log will indicate that the file has been updated.	Users can check the About boxes "Created on" to see if the date of the file has changed. Upgrading to version 4.0.3a corrects the problem.	VirusScan update problem	**High**	Bug discussed in newsgroups and Web sites.

[2] BUGTRAQ, April 27, 1999.
[3] BUGTRAQ, April 23, 1999.
[4] BUGTRAQ, May 4, 1999.
[5] BUGTRAQ, April 27, 1999.
[6] BUGTRAQ, May 3, 1999.
[7] CNET News.com, "Java bug crashes Windows 95,98," April 27, 1999.
[8] Nomad Mobile Research Centre Advisory, May 5, 1999.

Hardware/ Operating System	Equipment/ Software Name	Vulnerability/ Impact	Patches/Workarounds/Alerts	Common Name	Risk*	Attacks/Scripts
Novell[9]	Rconsole utility	Anyone with access to the sys:system\autoexec.nsf, sys:etc \netinfo.cy or sys:system\ldremote.ncf files can crack the rconsole password and gain remote access to the system.	Novell has no fixes planned and suggests that users remove the Remote Netware Loadable Module.	Rconsole password crack	Medium/ **High**	Bug discussed in newsgroups and Web sites. Exploit script has been published.
Oracle[10]	Oracle Intelligent Agent	An unauthorized user can run have Tcl commands run as root. It is then possible to fully compromise the system.	Workaround on current release is to *chown* the ORACLE_HOME/bin/oratclsh to oracle or other userid.	Oracle Intelligent Agent Tcl problem	**High**	Bug discussed in newsgroups and Web sites.
UNIX	BASH[11]	A number of vulnerabilities have recently been commented on in Listservs including a Buffer overflow in "make_cmd.c" and a directory problem. All these have been reported on older versions.	Updating to a new version corrects these vulnerabilities.	BASH overflow	**High** (if system is not updated to newer version of BASH)	Bug discussed in newsgroups and Web sites. Exploit script not required.

Special Note - There have been many reports of Shopping Cart systems exposing personal Credit Card numbers, Orders and other data. Many listservs and newsgroups have also discussed this problem. To date, the software vendors' response has been to refer users to "the manuals which describe in detail the steps to take to avoid" this type of mis-configuration problem. If you run one of these programs, you may wish to recheck the configuration to ensure that information is not available to unauthorized individuals.

*Risk is defined in the following manner:

High - A vulnerability that will allow an intruder to immediately gain privileged access (e.g., sysadmin, root) to the system. An example of this would be a vulnerability in which a sequence of instructions is sent to a machine by an unauthorized user and the machine responds with a command prompt.

Medium - A vulnerability that will allow an intruder immediate access to the system that is not privileged access. This allows the intruder the opportunity to continue the attempt to gain root access. An example would be a configuration error that allows an intruder to capture the password file.

Low - A vulnerability that provides information to an intruder that could lead to further compromise attempts or a Denial-of-Service (DoS) attack. The reader should note that while the DoS attack is deemed low from a threat potential, the frequency of this type of attack is very high. DoS attacks against mission-critical nodes are not included in this rating and any attack of this nature should instead be considered as a “High” threat.

[9] Infoworld, "Novell's Remote password falls victim to weak security measures," April 26, 1999.
[10] BUGTRAQ, April 30, 1999.
[11] BUGTRAQ, April 19, 1999.

Recent Exploit Scripts

The table below contains a representative sample of exploit scripts, identified between April 24 and May 9, 1999, listed by date of script, script name, script description, and comments. **Items listed in boldface/red (if any) are attack scripts for which vendors, security vulnerability listservs, or Computer Emergency Response Teams (CERTs) have not published workarounds or patches, or which represent scripts that hackers/crackers are utilizing**. During this period, 40 scripts, programs, and net-news messages containing holes or exploits were identified.

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
May 4, 1999	Saint-1.3.7.tar.gz	Gathers information on remote hosts by looking at network services.	
May 4, 1999	Tcpblast-19990504.tar.gz	Tool to probe networks and estimate network bandwidth.	
May 4, 1999	**Cgichk1.33.c**	**Program that checks for 53 Common Gateway Interface (CGI) vulnerabilities and, if any are found, will attempt to exploit the most common.**	
May 4, 1999	Gatescan.c	A class B/C network scanner with a number of command lines.	
May 4, 1999	Fav.c	Denial-of-Service exploit code used against Microsoft Internet Explore 5.0 favicon.ico bug.	
May 4, 1999	Edwards.txt	List of hard-coded administrative passwords for a number of JDEdwards applications.	
May 4, 1999	W00f.c	Exploit for obtaining root against machines running wu-ftpd. This code exploits the realpath() overflow.	
May 3, 1999	**NessusJ-alpha2.tar.gz**	**Java client for Nessus.**	
May 3, 1999	Uin2ip.pl	Perl script that resolves ICQ UINs to IP addressees.	
May 2, 1999	**Nmap-2.2-BETA3.tgz**	**Network-scanning tool that has a variety of scanning modes, including stealth, Xmas, and Null stealth. This version includes an optional GTK interface.**	
May 2, 1999	**Mns-v.75beta.tar.gz**	**Network scanner similar to nmap and sscan.**	
May 2, 1999	Icqget.pl	Program that allows an attacker to retrieve any file from a vulnerable ICQ-Webserver.	
May 1, 1999	Ethereal-0.6.1.tar.gz	Network protocol analyzer (sniffer).	
May 1, 1999	Fizzbounce.tar.gz	Bounces the connection of any HTTP proxy.	
May 1, 1999	Snoop2.c	Packet sniffer for SGI IRIX.	
May 1, 1999	Backdoor.c	Backdoor program that includes security features to insure backdoor is more difficult to discover and activate.	
May 1, 1999	Cgichk1.32.c	See entry for May 4, 1999	
April 30, 1999	Snort-1.0.tar.gz	Packet sniffer that places data in directories based on IP addresses of the captured packets.	
April 30, 1999	Mns-v.69beta.tar.gz	See entry for May 2, 1999	
April 29, 1999	Netxmon_0.6.tgz	Network sniffer with an X interface.	
April 29, 1999	Net-RawIP-0.06d.tar.gz	Perl module that manipulates raw Internet Protocol (IP) packets and Ethernet headers.	
April 29, 1999	**Scrack15.zip**	**Password cracker.**	
April 28, 1999	csmmail.c	Exploit code for CSMMail SMTP server resulting in root compromise.	

Date of Script **(Reverse Chronological Order)**	**Script Name**	**Script Description**	**Comments**
April 27, 1999	**Leetscan.tar.gz**	**Single host port scanner that is very fast.**	
April 27, 1999	Firewalk-0.99beta.tar.gz	Portscanner that attempts to identify what protocols are used on a given gateway.	
April 27, 1999	Mns-v.67beta.tar.gz	See entry for May 2, 1999.	
April 27, 1999	**Fawx.c**	**Program that sends oversized fragmented IGMP packets that cause systems to freeze or significantly degrade performance.**	
April 27, 1999	Xxploit.c	Exploit code for the Xfree sysmlink compromise.	
April 27, 1999	**ConFusion.zip**	**Win32 program that exploits vulnerabilities in Cold Fusion software.**	
April 27, 1999	Zone	This program exploits a vulnerability in Microsoft Outlook Express that results in unauthorized access to information (number of unread e-mails, etc.).	
April 26, 1999	**Lamescan-1.401b.tar.gz**	**Portscanner that conducts random scans and attempts to defeat warning programs by including a username with a port open request.**	
April 26, 1999	Detect-scans-0.80.tar.gz	Detects and logs portscans and a limited number of Denial-of-Service attacks.	
April 25, 1999	B4b0 #7	Electronic hacker magazine that includes a number of exploit scripts including: bouncer.c, GHCgi.c, FreeBSD rootkit and others.	
April 25, 1999	Netconfig.zip	Netware Trojan that presents the user with a failed log-in screen in an effort to have the user enter their password again.	
April 24, 1999	Egghack.tar.gz	Eggdrop userfile password cracker.	
April 24, 1999	Nskan-0.61b.tgz	Network scanner.	
April 24, 1999	Mailing.list.txt	Explanation of exploit that allows anyone to approve messages for a moderated mailing list that uses eGroups web site.	
April 24, 1999	**Qpop242.c**	**Exploit code for FreeBSD 2.2.5 and BSDi 2.1.**	
April 24, 1999	**Bsdi-imapd.c**	**Exploit code for imap2bis.**	
April 24, 1999	**Aixinfod.c**	**Exploit code for the AIX infod vulnerability leading to local root compromise.**	
April 24, 1999	**NBTscan**	**This program lists the IP address, NetBIOS name, logged-in user name and MAC address.**	

Script Analysis

This section will supply a short description of scripts that have been analyzed by various security professionals and organizations. If you or your organization wish to contribute, please send e-mail to nipc@fbi.gov with the subject line "CyberNotes Script Analysis." While this section will list only short descriptions, contributors are requested to include a full technical analysis of the script along with release instructions. The release categories are: releasable to anyone; limited releasability (originator-defined list of organizations); or provided for NIPC only. If you would like to receive a copy of the full technical analysis version of any summarized analysis, please send an e-mail listing the script name and requesting the full technical analysis. A member of the CyberNotes editorial team will contact you. All contributions will be credited to the contributing individual or organization unless otherwise requested.

Trends

Trends for this two week period:

1. Large number of probes for sites with ezmall2000 software installed.
2. Probes to port 1800 and 1945 continue.
3. Large numbers of web sites running the Cold Fusion Software have been hacked recently.
4. Probes looking for Cold Fusion sites continue.
5. Probes continue to look for machines with Back Orifice installed.
6. DoD has reported that the following methods have been used to compromise system in the last quarter (listed by number of successful pentrations): compromised passwords, vulnerability associated with Microsoft Frontpage and Windows NT, Post Office Protocol (POP), Common Gateway Interface (CGI), Telnet, CGI PHF, Internet Control Message Protocol (ICMP), and Internet Message Access Protocol (IMAP)

Viruses

A list of the top ten viruses infecting two or more sites as reported to various anti-virus vendors has been categorized into the two tables below. The first table list macro viruses, and the second table lists other viruses. Macro viruses have, historically, spread fastest due to their ability to be transferred by e-mail.

For the purposes of collecting and collating data, infections involving multiple systems at a single location are considered a single infection. The tables list the viruses by: ranking (number of sites affected), common virus name, type of virus (i.e., boot, file, macro, multi-partite), trends (based on number of infections during the last three months reported), and approximate date first found.

Note: Virus reporting is normally 6 to 8 weeks behind the first discovery of infection. With the number of viruses that appear each month, it is possible that a new virus will become widely distributed before the next edition of this publication. To limit the possibility of infection, readers are reminded to update their anti-virus packages, as soon as updates become available.

The viruses listed in the virus table infected over 300,000 machines in April, which represents an increase in the number of reported infections from the last prevalence table. When the CIH and Melissa viruses are removed from the count, the number of reported infections for the April timeframe continues to indicate an increase in viruses discovered over the last reporting period. The number 1 ranked virus (CIH) for April accounted for 300,000 reported infections worldwide, and the last virus listed in the tables infected 11. A total of 463 distinct viruses were reported this month, infecting over 2,000 sites (slight decrease from last months reporting). **Infection rates are based on number of machines infected, not number of sites**. This method reflects the way statistics are being gathered and reported by a number of anti-virus vendors.

Table 1 – Macro viruses:

Ranking	Common Virus Name	Type of Virus	Date First Reported
1	Melissa	Macro	March 1999
2	ColdApe	Macro	December 1998
3	CAP	Macro	April 1997
4	Class	Macro	September 1998
5	Ethan	Macro	February 1999
6	Npad	Macro	December 1996
7	Appender	Macro	May 1997
8	Concept	Macro	December 1996
9	Laroux	Macro	July 1997
10	Marker	Macro	February 1999

Table 2 – Other viruses:

Ranking	Common Virus Name	Type of Virus	Date First Reported
1	W95/CIH	File	July 1998
2	Form	Boot	September 1991
3	Parity_Boot	Boot	September 1993
4	AntiEXE	Boot	September 1994
5	AntiCMOS	Boot	October 1995
6	Junkie	Multi	July 1994
7	Empire.Monkey	Boot	July 1994
8	Sampo	Boot	January 1995
9	Stoned	Boot	September 1994
10	DelCMOS.B	Boot	January 1999

Win32/Ska (a.k.a HAPPY99) - This Trojan Horse continues to be reported to anti-virus vendors. This program has been distributed via e-mail, newsgroups and Web software distribution sites. Happy99.exe is the most common name of this Trojan horse, but reports have identified the use of other files names. When run, the program displays fireworks graphics and installs two files (ska.exe and ska.dll) in the System directory. The program then attempts to spam e-mail recipients and newsgroups to which the infected machine has sent or received messages. Sites with an e-mail filtering capability can filter messages with the header “X-Spanska: Yes.” Most major anti-virus vendors have included code in their latest data file updates to detect this Trojan horse program.